Updated: May 8, 2013   **Document ID:** 116133

Bias-Free Langua

Contents

Introduction

This document describes how to use a flow-based switched port analyzer (FSPAN) in order to capture filtered traffic on Cisco Catalyst switches that do not support VLAN access control list (VACL) capture.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Catalyst 3750-X Series Switches
- Cisco Catalyst 3560-X Series Switches
- Cisco Catalyst 3750-E Series Switches
- Cisco Catalyst 3560-E Series Switches
- Cisco Catalyst 2960-X Series Switches that run iplite license
- Cisco IOS® Release 12.2(44)SE and later

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Procedure

Cisco Catalyst 3750-X, 3560-X, 3750-E, 3560-E, and 2960-X (iplite license) switches do not support VACL capture; however, these switches do support flow-based SPAN and flow-based remote SPAN (RSPAN), which can achieve similar results to VACL capture.

Flow-based SPAN provides a mechanism to use specified filters in order to capture required data between end hosts.

You can attach three types of FSPAN access control lists (ACLs) to the SPAN session:

- IPv4 FSPAN ACL - filters IPv4 packets only.
- IPv6 FSPAN ACL- filters IPv6 packets only.
- MAC FSPAN ACL - filters non-IP packets only.

Security ACLs have higher priority than FSPAN ACLs on a switch. If you apply FSPAN ACLs and then add more security ACLs that cannot fit in hardware memory, the FSPAN ACLs are removed from memory in order to allow space for the security ACLs. A system message notifies user of this action, which is called unloading.

When space is again available, the FSPAN ACLs are added back to the hardware memory on the switch. A system message notifies user of this action, which is called reloading.

3750-X switches support up to two SPAN sessions, and FSPAN cannot avoid this limitation. FSPAN uses the same replication ASIC as a regular SPAN does.

This is an example of FSPAN use on a 3750-X switch:

```
3750X(config)#ip access-list extended FILTER
3750X(config-ext-nacl)#permit ip host 192.168.1.1 host 172.16.1.1
3750X(config-ext-nacl)#exit
3750X(config)#monitor session 1 source interface gi1/0/1 both3750X
(config)#monitor session 1 destination interface gi1/0/2 3750X
(config)#monitor session 1 filter ip access-group FILTER

3750X(config)##exit3750X#show monitor session
sh mon session  1
Session 1
---------
Type                    : Local Session
Source Ports            :
    Both                : Gi1/0/1Destination Ports     : Gi1/0/2
    Encapsulation       : Native
          Ingress       : Disabled
IP Access-group         : FILTER
```

Restrictions

- FSPAN is not supported on 3750, 3750G, 2950, 2960 and 2960-S switches.
- 2960-X that runs the iplite license only supports FSPAN.

- You can attach ACLs to only one SPAN or RSPAN session at a time.
- When no FSPAN ACLs are attached, FSPAN is disabled, and all traffic is copied to the SPAN destination ports.
- When at least one FSPAN ACL is attached, FSPAN is enabled.
- When you attach an empty FSPAN ACL to a SPAN session, it does not filter packets, and all traffic is monitored.
- Catalyst 3750 ports can be added as destination ports in an FSPAN session.
- VLAN-based FSPAN sessions cannot be configured on a stack that includes Catalyst 3750 switches.
- EtherChannels are not supported in an FSPAN session.
- FSPAN ACLs with TCP flags or the **log** keyword are not supported.
- Port-based FSPAN sessions can be configured on a stack that includes Catalyst 3750 switches as long as the session includes only Catalyst 3750-E ports as source ports. If the session has any Catalyst 3750 ports as source ports, the FSPAN ACL command is rejected.

Related Information

- Technical Support & Documentation - Cisco Systems

Trademarks

Supply Chain Transparency

Newsroom

Sitemap